UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/655,256	09/05/2000	Jeffrey T. Minnig	021768.1091	7727

7590 01/05/2005

Baker Botts L L P
2001 Ross Avenue
Dallas, TX 75201-2980

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	PAPER NUMBER
2134	

DATE MAILED: 01/05/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/655,256	MINNIG ET AL.	
	Examiner	Art Unit	
	Michael J Simitoski	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 August 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 September 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The response of 8/9/04 was received and considered.

2. Claims 1-21 are pending.

Response to Arguments

3. In light of applicant's amendments in the response filed 8/9/04, the objections to claims 3, 8, 13 & 18-20 and the rejections under 35 U.S.C. 112 ¶2 of claims 1, 3, 6, 9, 12, 16-17 & 19-21 are withdrawn. Further, the rejection of claim 14 (element 10 in the previous Office Action) is withdrawn.

4. Applicant's arguments filed 8/9/04 have been fully considered but they are not persuasive.

5. Applicant's arguments regarding the 35 U.S.C. §101 rejection of claim 21 (p. 11, ¶2), applicant sites O'Reilly v. Morse. This case relates to "signals for telegraphic purposes" of Morse code (1853) and is therefore unrelated to the computer-implemented method of the instant invention. The rejection is maintained.

6. Applicant's arguments regarding the rejection of claim 14 under 35 U.S.C. §102(b) (p. 11, ¶4 – p. 13, ¶1) have been considered, but are not persuasive. Applicant argues (p. 12, last ¶) that Borella fails to disclose "the decoded port command [being] modified by overriding the client internal IP address within the decoded port command with a client external IP address retrieved from the header". Applicant is directed to p. 15 (first figure) of Borella where the port command (Src: 10.0.0.2) is modified by overriding (p. 15, ¶3) the client internal IP address (Src: 10.0.0.2) within the decoded port command with a client external IP address (Src:

149.112.240.55) retrieved from the header. The outer IP header is stripped off, overriding the client internal IP address with the client external IP address. Further, applicant argues (p. 17, ¶2-3) that Stallings fails to disclose a data payload including an encoded port command including a client internal IP address and a client port number and states that the Office Action concedes that the client port number of Stallings is "contained in the TCP/IP header". However, this is a standard feature of the OSI model of networking, wherein an IP header is enclosed in a TCP header, hence TCP/IP (see TCP/IP architecture overview).

7. Applicant's arguments regarding the rejection of claim 1 under 35 U.S.C. §103(a) (p. 13, ¶2 – p. 14, ¶1) have been considered, but are not persuasive. Applicant argues (p. 13, ¶3) that Stallings does not disclose an "encoded port command" having a "client internal IP address and a client port number". The port command/original packet is encoded (encapsulated using binary) in a new packet (p. 179, Fig. 6.9(b)). Applicant is directed to p. 179 where Stallings discloses a TCP/IP packet with an original packet encapsulated in a second packet. Specifically, the original header contains the client internal IP address and the client port number, as per definition of a TCP/IP packet (evidenced by the previously-cited "TCP/IP Illustrated" excerpt by Stevens). Further, in network communication, a source and destination are specified. A client can be either the source or a destination of a packet and as well can act as a server to other servers/clients. Applicant argues (p. 14, ¶1) that Stallings does not contemplate establishing a second channel based on the modified port command. However, Stallings is cited for teaching encapsulation, where a packet is encapsulated in another packet for transmission between second nodes, part of the packet being used for transmission between certain nodes and another part for transmission between different nodes (p. 183, Fig. 6.10(c)) shows this. While Stallings lacks a "channel", the

packet is still used for multiple connections (Host->Security Gateway->Security Gateway->Host, for example). It is for this reason Stallings discloses a port command having an internal IP address and a client data port number. If applicant intends to rely on the PORT command being "encrypted", rather than the broader "encoded", then this limitation must be explicit in the claim.

8. Applicant's arguments regarding the rejection of claim 6 under 35 U.S.C. §103(a) (p. 14, ¶2) have been considered, but are not persuasive. Applicant argues that Stallings fails to disclose a communication packet having a header, and a data payload having an encoded port command having a server internal IP address and a server data port number. As stated in the previous paragraph, Stallings discloses an encapsulated packet, which contains a header and a data payload having an encoded port command (original header) having a server internal IP address and a server port number. A server can be either the source or a destination of a packet and as well can act as a client to other servers/clients.

9. Applicant's arguments regarding the rejection of claim 17 under 35 U.S.C. §103(a) (p. 14, ¶3) have been considered, but are not persuasive. Applicant argues that Stallings fails to disclose a communication packet having a header, and a data payload having an encoded port command having a server internal IP address and a server data port number. Stallings discloses a port command/original packet being encoded (encapsulated using binary) in a new packet (p. 179, Fig. 6.9(b)). Applicant is directed to p. 179 where Stallings discloses a TCP/IP packet with an original packet encapsulated in a second packet. Specifically, the original header contains the client internal IP address and the client port number, as per definition of a TCP/IP packet (evidenced by the previously-cited "TCP/IP Illustrated" excerpt by Stevens). Further, in network

communication, a source and destination are specified. A server can be either the source or a destination of a packet and as well can act as a client to other servers/clients.

10. Applicant's arguments regarding the rejection of claim 20 under 35 U.S.C. §103(a) (p. 15, ¶2 – p. 16, ¶3) have been considered, but are not persuasive. Applicant argues that the rejection of claim 20 is improper because it is improper "to use hindsight having read the Applicant's disclosure to arrive at an obviousness rejection" and "to use the claimed invention as an instruction manual or template to piece together the teachings" (p. 15, ¶2), however applicant has not cited any specific reasons why the motivation provided in the previous Office Action fails to apply. Applicant is directed to the previous Office Action (pp. 10-12) where the Examiner has cited motivation for combining the Stallings, Egevang, Phifer and Bellovin.

11. Applicant's arguments regarding the rejection of claims 5 & 10 under 35 U.S.C. §103(a) (p. 16, ¶4-5) have been considered, but are not persuasive. Applicant argues that claims 5 & 10 are patentably distinguishable from the prior art based on their dependence on claims 1 & 6. See the Examiner's response to arguments regarding claims 1 & 6 above.

12. Applicant's arguments regarding the rejection of claims 15 & 16 under 35 U.S.C. §103(a) (p. 17, ¶4) have been considered, but are not persuasive. Applicant argues that claims 15 & 16 are patentable by relying on the patentability of claim 14. See the Examiner's response to arguments regarding claim 14 above.

13. Applicant's arguments regarding the rejection of claim 11 under 35 U.S.C. §103(a) (p. 18, ¶1) have been considered, but are not persuasive. Applicant argues that Stallings fails to disclose "using [a] modified port command to establish a data socket between first and second peers." As stated in the Office Action, Borella discloses a method of network address

translation, where the source addresses and ports are exchanged transit (pp. 15-16). Microsoft is cited for teaching that when a first node replies to a second node, it must create a modified port command so the reply (packet) will be delivered to the correct destination (p. 1).

Claim Rejections - 35 USC § 101

14. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

15. Claim 21 is rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The subject matter being claimed is a "signal" which is none of a process, machine, manufacture or composition of matter.

Claim Rejections - 35 USC § 102

16. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

17. Claim 14 is rejected under 35 U.S.C. 102(b) as being anticipated by "Distributed Network Access Translation" by Borella et al. (Borella). Borella discloses encoding a port command including a client internal IP address/Src of outer header and client port number/Src port (p. 15, first Fig.), generating a dual channel communication packet having a header and a data payload (p. 15) with a server external IP address/Des of inner header, server port number/Dst port, client internal IP address/Src in outer header and client port number/Src port (p.

15). The packet is sent to the server and the port command is decoded/read (p. 15). Borella discloses modifying the decoded port command by overriding the client internal IP address/Src in outer header with the client external IP address/Src in inner header and establishing a data socket (data flow) between the server and the client (p. 15).

Claim Rejections - 35 USC § 103

18. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

19. Claims 1-4, 6-9 & 17-20, as best understood, are rejected under 35 U.S.C. 103(a) as being unpatentable over Network Security Essentials, Applications and Standards by Stallings in view of "The IP Network Address Translator (NAT)" by Egevang et al. (Egevang) in view of "IP Security and NAT: Oil and Water?" by Phifer in further view of "Firewall-Friendly FTP" (RFC 1579) by Bellovin.

Regarding claims 1 & 3, Stallings discloses a communication packet having a header/outer header and a data payload/original packet, the data payload including a port command/original packet including a client internal IP address/source address (p. 179, Fig. 6.9(b) & p. 180) and a client port number/port (contained in an TCP/IP header) and a header/outer and inner packet (p. 179). Stallings further discloses decoding the port command/original packet (p. 180, step 3). Stallings lacks a header having a client external IP address and a translation module operable to retrieve the client external IP address from the

header and to generate a modified port command including the external IP address, where the server is operable to establish a second channel based on the modified port command. However, Egevang teaches a protocol (NAT) to reduce IP address depletion (p. 1) (NAT is commonly used today and is incorporated with routers, as in Fig. 2). NAT states that when sending a packet from a source behind a router (Stub A) to a destination behind another router (Stub B), a packet will contain Stub A's internal address and Stub B's global address (Fig. 2). Stub A's local address will be readdressed to the global address at Stub A's router and sent to Stub B's global address (Fig. 2). At Stub B's router, the destination address will be replaced with Stub B's internal address and forwarded to stub B and a similar method is used in the reverse direction (Fig. 2 and p. 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Stallings and Egevang to use IPSec with NAT and route the packet according to the same transformations as occurred between Stubs A and B. One of ordinary skill in the art would have been motivated to perform such a modification because NAT is known to reduce the problems associated with IP address depletion (p. 1) and because a skilled artisan in network architecture knows of NAT's widespread use and acceptance. In combination, a client external IP address (translated at the stub router from the internal address) is included in the header. Further, Phifer teaches that to avoid problems with locating endpoints in IPSec, one can perform network address translation outside IPSec (p. 2). In doing so, the inner packet's internal client address is replaced with the client's external address (p. 2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decode the port command and replace the client internal IP address with the client external IP address found in the header (NAT translating outside IPSec). One of

ordinary skill in the art would have been motivated to perform such a modification to avoid problems with locating endpoints in IPSec, as taught by Phifer (p. 2). Stallings, as modified above, lacks a *second* channel being established and lacks specifically a server performing the functions. However, Bellovin teaches that FTP uses two channels, a control channel and a data channel where the control channel is used to negotiate the connection and the data channel uses that second connection to transfer data (pp. 1-2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable an FTP server to perform the functions described above and to establish a second connection based on the modified port command. One of ordinary skill in the art would have been motivated to perform such a modification to support the well-known FTP protocol, as taught by Bellovin (pp. 1-2).

Regarding claim 2, the examiner takes Official Notice that packet filters (hardware and software) are old and well established in the art of computer security as a method of preventing potentially harmful traffic from entering a network. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to include a packet filtering server firewall in the server. One of ordinary skill in the art would have been motivated to perform such a modification to prevent potentially harmful traffic from entering the server. This advantage is well known to those skilled in the art.

Regarding claim 4, Stallings, as modified above, discloses FTP communication conducted over a secure tunnel (Stallings, p. 179 & Egevang, pp. 1-10).

Regarding claim 6-9, the claims are substantially equivalent to claims 1-4, respectively. Therefore, claims 6-9 are rejected under similar rationale.

Regarding claim 17, Stallings discloses encoding a port command/original packet including a client internal IP address/source address (p. 179, Fig. 6.9(b)) and a client port number/port (contained in an TCP/IP header), generating a communication packet having a header/outer header and a data payload/original packet, the data payload including the encoded port command/original packet (Fig. 6.9(b)), transmitting the packet between a server/destination and the client/source (p. 180), decoding the port command/original packet (p. 180, step 3) and establishing a data socket (data flow) between the server/destination and the client/source (p. 180, step 3). The header includes a server external IP address/destination firewall address and a server port (TCP header) and a client internal IP address/source address and port (TCP header) (pp. 180-181). Stallings lacks explicitly overriding the client internal IP address/source address within the decoded port command/original packet with the client external IP address retrieved from the header. However, Egevang teaches a protocol (NAT) to reduce IP address depletion (p. 1) (NAT is commonly used today and is incorporated with routers, as in Fig. 2). NAT states that when sending a packet from a source behind a router (Stub A) to a destination behind another router (Stub B), a packet will contain Stub A's internal address and Stub B's global address (Fig. 2). Stub A's local address will be readdressed to the global address at Stub A's router and sent to Stub B's global address (Fig. 2). At Stub B's router, the destination address will be replaced with Stub B's internal address and forwarded to stub B and a similar method is used in the reverse direction (Fig. 2 and p. 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Stallings and Egevang to use IPSec with NAT and route the packet according to the same transformations as occurred between Stubs A and B. One of ordinary skill in the art would have been motivated to

perform such a modification because NAT is known to reduce the problems associated with IP address depletion (p. 1) and because a skilled artisan in network architecture knows of NAT's widespread use and acceptance. Further, Phifer teaches that to avoid problems with locating endpoints in IPSec, one can perform network address translation outside IPSec (p. 2). In doing so, the inner packet's internal client address is replaced with the client's external address. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decode the port command and replace the client internal IP address with the client external IP address (NAT translating outside IPSec). One of ordinary skill in the art would have been motivated to perform such a modification to avoid problems with locating endpoints in IPSec, as taught by Phifer (p. 2). As modified, Stallings lacks "transmitting a passive command to the server". However, Bellovin teaches that using the PASV (passive command) to initiate an FTP session reduces problems associated with FTP through firewalls (p. 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to transmit a passive command/PASV to the server. One of ordinary skill in the art would have been motivated to perform such a modification to reduce problems associated with FTP communication through firewalls, as taught by Bellovin (p. 1).

Regarding claims 18 & 19, Stallings, as modified above, discloses readdressing the client internal IP address within the header with the client external IP address at a client firewall and readdressing the server external IP address within the header with the server internal IP address at a server firewall (Stallings, p. 183, Fig. 6.10(b) & Egevang, p. 3).

Regarding claim 20, Stallings discloses establishing a channel between a server and a client (p. 183, Fig. 6.10(b)), identifying a first end point/inner packet at a first one of a server and

a client (two hosts), the first end point including a first portion/destination and a second portion/source (p. 180), encoding the first end point in a secure format (encapsulate with new IP header) (p. 180), transmitting the transmission packet over the external network in the channel (p. 180, step 2) and receiving the transmission packet at the other client or server (p. 180, step 3). Stallings lacks explicitly translating the private address in the address header into a public address for transmitting over the external network. However, Egevang teaches a protocol (NAT) to reduce IP address depletion (p. 1) (NAT is commonly used today and is incorporated with routers, as in Fig. 2). Egevang teaches that when sending the data packet, the private address must be translated to a global address (Fig. 2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to translate the private address to a public/global address. One of ordinary skill in the art would have been motivated to perform such a modification to use network address translation to use a private (non-globally routable) IP address and hence reduce IP address depletion, as taught by Egevang (pp. 1-3). As modified, Stallings lacks modifying the end point by replacing the first portion in the decoded end point with the public address in the address header. However, Phifer teaches that to avoid problems with locating endpoints in IPSec, one can perform network address translation outside IPSec (p. 2). In doing so, the inner packet's internal client address is replaced with the client's external address. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to replace the first portion with the public address in the address header. One of ordinary skill in the art would have been motivated to perform such a modification to avoid problems with locating endpoints in IPSec, as taught by Phifer (p. 2). As modified, Stallings lacks the initial channel being a control channel and establishing a data channel

between the client and the server using the modified end point. However, Bellovin teaches that FTP uses two channels, a control channel and a data channel where the control channel is used to negotiate the connection and the data channel uses that second connection to transfer data (pp. 1-2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to enable an FTP server to perform the functions described above and to establish a second connection based on the modified port command. One of ordinary skill in the art would have been motivated to perform such a modification to support the well-known FTP protocol, as taught by Bellovin (pp. 1-2).

20. Claims 5 & 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings, Egevang, Phifer and Bellovin, as applied to claims 1 & 6 above, in further view of "SMTP Service Extension for Secure SMTP over TLS" (RFC 2487) by Hoffman.

Regarding claim 5, Stallings, as modified above, lacks SSL encryption technology as the codec. However, Hoffman teaches that SSL is a popular mechanism for enhancing TCP communications with privacy and authentication (p. 1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to choose SSL encryption technology to encrypt the port command/inner header. One of ordinary skill in the art would have been motivated to perform such a modification to enhance communications with privacy (encryption), as taught by Hoffman (p. 1).

Claim 10 is substantially equivalent to claim 5. Therefore, claim 10 is rejected under similar rationale.

21. Claims 14-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Stallings, Egevang and Phifer.

Regarding claim 14, Stallings discloses encoding a port command/original packet including a client internal IP address/source address (p. 179, Fig. 6.9(b)) and a client port number/port (contained in an TCP/IP header), generating a communication packet having a header/outer header and a data payload/original packet, the data payload including the encoded port command/original packet (Fig. 6.9(b)), transmitting the packet between a server/destination and the client/source (p. 180), decoding the port command/original packet (p. 180, step 3) and establishing a data socket (data flow) between the server/destination and the client/source (p. 180, step 3). The header includes a server external IP address/destination firewall address and a server port (TCP header) and a client internal IP address/source address and port (TCP header) (pp. 180-181). Stallings lacks explicitly overriding the client internal IP address/source address within the decoded port command/original packet with the client external IP address retrieved from the header. However, Egevang teaches a protocol (NAT) to reduce IP address depletion (p. 1) (NAT is commonly used today and is incorporated with routers, as in Fig. 2). NAT states that when sending a packet from a source behind a router (Stub A) to a destination behind another router (Stub B), a packet will contain Stub A's internal address and Stub B's global address (Fig. 2). Stub A's local address will be readdressed to the global address at Stub A's router and sent to Stub B's global address (Fig. 2). At Stub B's router, the destination address will be replaced with Stub B's internal address and forwarded to stub B and a similar method is used in the reverse direction (Fig. 2 and p. 3). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to combine the teachings of Stallings and

Egevang to use IPSec with NAT and route the packet according to the same transformations as occurred between Stubs A and B. One of ordinary skill in the art would have been motivated to perform such a modification because NAT is known to reduce the problems associated with IP address depletion (p. 1) and because a skilled artisan in network architecture knows of NAT's widespread use and acceptance. Further, Phifer teaches that to avoid problems with locating endpoints in IPSec, one can perform network address translation outside IPSec (p. 2). In doing so, the inner packet's internal client address is replaced with the client's external address. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to decode the port command and replace the client internal IP address with the client external IP address (NAT translating outside IPSec). One of ordinary skill in the art would have been motivated to perform such a modification to avoid problems with locating endpoints in IPSec, as taught by Phifer (p. 2).

Regarding claims 15 & 16, Stallings, as modified above, discloses readdressing the client internal IP address within the header with the client external IP address at a client firewall and readdressing the server external IP address within the header with the server internal IP address at a server firewall (Stallings, p. 183, Fig. 6.10(b) & Egevang, p. 3).

22. Claims 11-13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Borella in view of "Unicast Routing Overview" by Microsoft.

Regarding claim 11, Borella discloses a packet being sent (outbound) and received (inbound) (pp. 15-16). The inner IP header shows that when sending a packet from PC2 (10.0.0.2) to its router (10.0.0.1), the outbound packet contains 10.0.0.2 as the source address and

10.0.0.1 as the destination address (p. 15). Similarly, when the packet is returned from the router to PC2, the inbound packet contains 10.0.0.1 as the source address and 10.0.0.2 as the destination address (p. 16). The ports are addressed in the same reversible manner, depending on whether the packet is inbound or outbound (pp. 15-16). Microsoft teaches that unicast routing consists of determining a destination address and transmitting an IP packet from a host to a destination based on that destination address (p. 1). Therefore, during any receive/reply TCP/IP transaction, a receiver/second peer receives a packet from a sender/first peer including a header/IP header and a port command/packet with TCP ports encoded therein. Upon replying to the sender (response), a modified port command is created including a first peer IP address/source IP in place of the second peer IP address/destination IP (swapping source and destination IP addresses and ports) and a connection is established between the first and second peers (data sent from original receiver to original sender). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use the unicast routing, as taught by Microsoft (p. 1) to accomplish a receive/reply (standard TCP/IP transaction) as taught by Borella. One of ordinary skill in the art would have been motivated to perform such a modification to transfer data from a source to a destination, as taught by Microsoft (p. 1).

Regarding claims 12 & 13, the claims are substantially equivalent to claim 11. Therefore, claims 12 & 13 are rejected under similar rationale.

Conclusion

23. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

a. "MOVEit DMZ" by Lampe is cited for teaching decrypting a PORT command, retrieving an external IP address, modifying a received PORT command with the external IP address and creating a data socket over a separate channel using the modified PORT command (p. 7). *The Standard Network reference specifically teaches passive mode; in active mode, the graphic on page 7 would have the first two messages sent from the client and the last connection being sent from the server to the client.*

b. "KTELNET Version 2.01" by Nystrom et al. is cited for teaching that to solve the problem of using NAT with FTP. KTELNET discloses that Ktelnet must figure out the IP-address that the server sees you from (your external address) (p. 13). Specifically, the Kerberos Client must supply its own IP-address to the server in a Kerberos packet and the address supplied must be the same address that the Kerberos Server sees the client as.

c. "How do I user FTP with SSL behind a NAT" by Indy Project, "IP Masquerading with Linux" by Kostick, "FTP and NAT: solutions" by Leledy, "FTP/TLS Friendly Firewalls" by Ford-Hutchinson, "The Trouble with NAT" by Phifer, "Transparent Routing between Ipv4/Ipv6 Networks" by Baptiste et al., "Network Address Translation – Protocol Translation (NAT-PT)" by Tsirtsis et al., "Network Address Translation" by Wikipedia and "An SNMP Application Level Gateway for Payload Address Translation" by Raz et al. are cited for teaching an Application Layer Gateway replacing a client internal IP address in a PORT command with a client's external IP address (see emphasized portions).

d. "Forwarding FTP" by SSH, "FTP Active and Passive Modes" by Mail-Production.com, "Analysis of the File Transfer Control Protocol (FTP)" by

Oppenheimer, "Security>> 3. NAT Routers" by Broadband Reports and "File Transfer Protocol (FTP)" by Postel et al. are cited for teaching NAT and FTP and specifically that standard FTP uses a PORT command in active mode where a client sends its address to a server, which then creates a data socket via a second channel back to the client.

e. U.S. Patent 6,415,329 is cited for teaching routing packets from a client to a server through multiple NAT interfaces (Fig. 14).

f. "When NAT becomes NOT" by Justin teaches the problem with NAT and FTP.

24. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

25. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (571) 272-3841. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached at (571) 272-3838.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(571)273-3841 (Examiner's fax, for informal or draft communications, please label "PROPOSED" or "DRAFT")

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571) 272-2100.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
December 21, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100